REGLAMENTO DE LA LEY DE FIRMAS Y CERTIFICADOS DIGITALES (LEY 27269)..

DECRETO SUPREMO Nº 019-2002-JUS

EL PRESIDENTE DE LA REPÚBLICA
CONSIDERANDO:
Que, mediante Ley Nº 27269, se aprobó la Ley de Firmas y Certificados Digitales; disponiendo en su artículo 16º, que el Poder Ejecutivo reglamentará la citada Ley.
Que, mediante Ley Nº 27310, se modificó el artículo 11º de la referida Ley, en el sentido, que los Certificados de Firmas Digitales emitidos por Entidades Extranjeras tendrán la misma validez y eficacia jurídica reconocidas en la Ley Nº 27269, siempre y cuando, tales certificados sean reconocidos por la Autoridad Administrativa Competente;
Que, la Autoridad Administrativa Competente de conformidad con lo establecido en el artículo 15º de la Ley Nº 27269, será determinada por el Poder Ejecutivo, estableciendo sus funciones;
Que, por Resolución Suprema Nº 098-2000-JUS, se designó la Comisión Multisectorial encargada de elaborar el Reglamento de la Ley de Firmas y Certificados Digitales;
Que, mediante Resolución Suprema Nº 280-2001-JUS, se dio por concluida la labor de la Comisión Multisectorial citada en el considerando anterior, publicándose el Proyecto de Reglamento en el Diario Oficial para los comentarios y sugerencias del caso;
Que, el Ministerio de Justicia ha cumplido con evaluar los diversos comentarios y sugerencias recibidas, incorporándose los aportes pertinentes que han enriquecido y mejorado el Reglamento;
Que, es necesario aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley Nº 27269, que permitirá poner en práctica y difundir en el más breve plazo el uso de las Firmas Electrónicas, así como las Firmas y Certificados Digitales, a través de la adecuada regulación de las Entidades de Certificación y de las Entidades de Registro o Verificación;
De conformidad con lo dispuesto en el inciso 8) del artículo 118º de la Constitución Política del Perú;
DECRETA:
Artículo 1º .- Aprobar el Reglamento de la Ley de Firmas y Certificados Digitales - Ley Nº 27269, que consta de tres (3) Títulos, cincuenta (50) artículos y dos (2) Disposiciones Finales..
Artículo 2º .- Designar al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente, conforme a lo establecido en el artículo 15º de la Ley Nº 27269.
Artículo 3º .- El presente Decreto Supremo será refrendado por el Presidente del Consejo de Ministros y por el Ministro de Justicia.
Dado en la Casa de Gobierno, a los diecisiete días del mes de mayo del año dos mil dos.
RAÚL DIEZ CANSECO TERRY
Primer Vicepresidente de la República
Encargado del Despacho Presidencial
ROBERTO DAÑINO ZAPATA
Presidente del Consejo de Ministros
FERNANDO ROSPIGLIOSI C.
Ministro del Interior
Encargado de la Cartera de Justicia

Reglamento de la Ley de Firmas y Certificados Digitales Ley Nº 27269

TÍTULO I
NORMAS GENERALES

CAPÍTULO I

Artículo 1º .- Objeto
El Reglamento regula, para el sector público y privado, la utilización de firmas electrónicas en mensaje de datos y documentos electrónicos, generadas bajo la Infraestructura Oficial de Firma Electrónica comprendiendo el régimen de acreditación y supervisión de las entidades de certificación, así como de las entidades de registro o verificación, establecidas en la Ley Nº 27269 -Ley de Firmas y Certificados Digitales-, modificada en su artículo 11º por la Ley Nº 27310. Cuando en el Reglamento se haga referencia a la Ley, debe entenderse referida a la Ley Nº 27269, Ley de Firmas y Certificados Digitales. Cuando se mencione el Reglamento debe entenderse referido al presente Reglamento, de la Ley Nº 27269..Las firmas electrónicas aprobadas por la autoridad administrativa competente,
tienen, desde su aprobación los mismos efectos que las firmas generadas bajo la Infraestructura Oficial de Firma Electrónica conforme a lo establecido en el Reglamento.

Artículo 2º .- Principio de la autonomía de la voluntad
Las disposiciones contenidas en el Reglamento no restringen la autonomía privada para el uso de otras firmas electrónicas generadas fuera de la Infraestructura Oficial de Firma Electrónica, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en el artículo 1º de la Ley.

Artículo 3º .- Régimen de servicios de certificación
La prestación de servicios de certificación así como los de registro o verificación se sustenta en el principio de libre competencia y en el marco de una economía social de mercado.

Artículo 4º .- Definiciones
Para efectos del Reglamento, entiéndase por:
Acreditación.- Proceso a través del cual la autoridad administrativa competente, previo cumplimiento de las exigencias establecidas en la Ley, faculta a las entidades solicitantes reguladas en el Reglamento a prestar los servicios solicitados en el marco de la Infraestructura Oficial de Firma Electrónica.
Agente automatizado.- Procesos y equipos programados para atender requerimientos predefinidos y dar una respuesta automática sin intervención humana, en dicha fase.
Algoritmo.- Conjunto ordenado y finito de operaciones matemáticas que permiten hallar la solución a un problema.
Autenticación.- Proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.
Autoridad Administrativa Competente.- Organismo público responsable de acreditar a las entidades de certificación y a las entidades de registro o verificación, de reconocer los estándares tecnológicos aplicables en la Infraestructura Oficial de Firma Electrónica, de supervisar dicha Infraestructura, y las otras funciones señaladas en el Reglamento o aquéllas que requiera en el transcurso de sus operaciones.
Certificado digital.- Documento electrónico generado y firmado digitalmente por una entidad de certificación el cual vincula un par de claves con una persona natural o jurídica confirmando su identidad.
Certificación Cruzada.- Acto por el cual una entidad de certificación acreditada reconoce la corrección y validez de un certificado digital emitido por otra entidad de certificación, sea nacional, extranjera o internacional, previa.autorización de la autoridad administrativa competente; y asume tal certificado
como si fuera de propia emisión, bajo su responsabilidad.
Clave privada.- En un sistema de criptografía asimétrica, es aquella que se emplea para generar una firma digital sobre un mensaje de datos y es mantenida en reserva por el titular de la firma digital.
Clave pública.- En un sistema de criptografía asimétrica, es aquella usada

por el destinatario de un mensaje de datos para verificar la firma digital puesta en dicho mensaje y que puede ser conocida por cualquier persona.
Código de verificación.- Secuencia de bits de longitud fija obtenida como resultado de procesar un mensaje de datos con un algoritmo, de tal manera que: (1) El mensaje de datos produzca siempre el mismo código de verificación cada vez que se le aplique dicho algoritmo. (2) Sea improbable, a través de medios técnicos, que el mensaje de datos pueda ser derivado o reconstruido a partir del código de verificación producido por el algoritmo. (3) Sea improbable que, por medios técnicos, se pueda encontrar dos mensajes de datos que produzcan el mismo código de verificación al usar el mismo algoritmo.
Criptografía asimétrica.- Es una técnica basada en el uso de un único par de claves; una clave privada y una clave pública relacionadas matemáticamente entre sí de tal manera que una no pueda operar sin la otra y de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada.
Declaración de prácticas de certificación.- Documento oficialmente presentado por una entidad de certificación a la Autoridad Administrativa Competente, mediante la cual define sus Prácticas de Certificación.
Declaración de Prácticas de Registro o Verificación: Documento oficialmente presentado por una Entidad de Registro o Verificación a la Autoridad Administrativa Competente, mediante la cual define sus Prácticas de Registro o Verificación.
Depósito de certificados digitales.- Sistema de almacenamiento y recuperación de certificados digitales, así como de la información relativa a éstos, disponible por medios telemáticos.
Destinatario.- Persona designada por el iniciador para recibir un mensaje de datos o un documento electrónico, siempre y cuando no actúe a título de intermediario.
Documento Electrónico.- Conjunto de datos basados en bits o impulsos electromagnéticos, elaborados, generados, transmitidos, comunicados y archivados a través de medios electrónicos, ópticos o cualquier otro análogo.
Entidad de Certificación.- Persona jurídica que presta indistintamente servicios de producción, emisión, gestión, cancelación u otros servicios inherentes a la certificación digital. Asimismo, puede asumir las funciones de registro o verificación..**Entidad de Certificación Extranjera.-** La que no se encuentra domiciliada en el país, ni inscrita en los Registros Públicos del Perú, conforme a la legislación de la materia.
Entidad de Registro o Verificación.- Persona jurídica encargada del levantamiento de datos, la comprobación de éstos respecto a un solicitante de certificado digital, la aceptación y autorización de las solicitudes para la emisión de certificados digitales, así como de la aceptación y autorización de las solicitudes de cancelación de certificados digitales.
Estándares Técnicos Internacionales.- Requisitos de orden técnico y de uso internacional que deben observarse en las Prácticas de Certificación para garantizar el intercambio de claves públicas, y la emisión de firmas y certificados digitales, mediante criptografía asimétrica.
Estándares Técnicos Nacionales.- Estándares técnicos aprobados mediante Normas Técnicas Peruanas por la Comisión de Reglamentos Técnicos y Comerciales - CRT del INDECOPI, en su calidad de Organismo Nacional de Normalización.
Firma digital.- Aquella firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido.
Firma electrónica.- Cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse, autenticar y garantizar la integridad de un documento electrónico o un mensaje de datos cumpliendo todas o algunas de las funciones características de una firma manuscrita.
Reconocimiento.- Proceso a través del cual la autoridad administrativa competente, equipara y reconoce oficialmente a las entidades de certificación extranjeras.

Infraestructura Oficial de Firma Digital.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente en el marco de la Infraestructura Oficial de Firma Electrónica mediante el uso de tecnología de firma digital, en la que participan entidades de certificación y entidades de registro o verificación acreditadas ante la autoridad administrativa competente.
Infraestructura Oficial de Firma Electrónica.- Sistema confiable, acreditado, regulado, y supervisado por la autoridad administrativa competente constituido por programas, equipos, estándares, políticas, procesos, procedimientos u otros recursos que permiten la generación de firmas electrónicas y que garantizan la autenticación e integridad de los documentos electrónicos.
Iniciador.- Persona que haya actuado por su cuenta o a cuyo nombre se haya actuado para enviar o generar un mensaje de datos antes de ser archivado, pero que no haya actuado a título de intermediario..
Integridad.- Característica que indica que un mensaje de datos o un documento electrónico no han sido alterados desde la transmisión por el iniciador hasta su recepción por el destinatario.
Intermediario.- Persona que, actuando por cuenta de otra, envía, recibe o archiva un mensaje de datos o presta otro servicio respecto de él.
Medios Telemáticos.- Conjunto de bienes y elementos técnicos informáticos que en unión con las telecomunicaciones permiten la generación, procesamiento, transmisión, comunicación y archivo de datos e información.
Mensaje de datos.- Es la información generada, transmitida, recibida, archivada, comunicada por medios electrónicos, ópticos o cualquier otro análogo; tales como, el intercambio electrónico de datos (EDI, por sus siglas en inglés), el correo electrónico, el telegrama, el télex, el telefax, entre otros.
Neutralidad Tecnológica.- Principio que fomenta la creación y uso de diversas tecnologías, sin preferir, restringir, ni discriminar a ninguna de ellas.
Par de claves.- En un sistema de criptografía asimétrica, comprende una clave privada y su correspondiente clave pública, ambas asociadas matemáticamente.
Servicio de Valor Añadido en Firmas Electrónicas.- Servicio complementario a las funciones de certificación, verificación o registro al interior de la Infraestructura Oficial de Firma Electrónica, como fuera de ella.
Tiempo Universal Coordinado (UTC).- Hora relacionada con el Meridiano de Greenwich.
Titular de certificado digital.- Persona natural o jurídica a quien se le atribuye de manera exclusiva un certificado digital.
Titular de firma digital.- Persona natural a quien se le vincula de manera exclusiva con un mensaje de datos firmado digitalmente utilizando su clave privada.
Por excepción, en el caso de firmas digitales generadas a través de agentes automatizados, se considera titular de la firma digital a la persona natural o jurídica titular del certificado digital a partir del cual se generan dichas firmas digitales.

CAPÍTULO II
VALIDEZ Y EFECTOS JURÍDICOS DE LAS FIRMAS Y DOCUMENTOS ELECTRÓNICOS

Artículo 5º .- Firmas en la Infraestructura Oficial de Firma Electrónica
Toda firma electrónica añadida o asociada lógicamente a un mensaje de datos o a un documento electrónico y generada bajo la Infraestructura Oficial de Firma Electrónica, cumple con lo dispuesto en la Ley y el Reglamento..
Artículo 6º .- Validez de otras firmas electrónicas
Para efectos de la manifestación de voluntad, las firmas electrónicas añadidas o asociadas lógicamente a un mensaje de datos o un documento electrónico y generadas fuera de la Infraestructura Oficial de Firma Electrónica tendrán la misma validez y eficacia jurídica que las firmas manuscritas, siempre que sean acreditadas o reconocidas por la autoridad administrativa competente.
Artículo 7º .- Documentos Firmados Electrónicamente como medio de prueba
Las firmas electrónicas así como los mensajes de datos y documentos firmados

electrónicamente podrán ser admitidas como prueba en toda clase de procesos o procedimientos. El Juez podrá solicitar a la autoridad administrativa competente el nombramiento de un perito especializado en firmas electrónicas.

Artículo 8º .- Presunciones acerca de las firmas electrónicas bajo la Infraestructura Oficial de Firma Electrónica

Tratándose de mensaje de datos o documentos firmados electrónicamente con firmas generadas bajo la Infraestructura Oficial de Firma Electrónica, se presume que el documento o mensaje de datos fue enviado y firmado por su titular, de manera tal que identifica y vincula al firmante, y garantiza la autenticación e integridad del mismo.

Las disposiciones y presunciones del Reglamento no excluyen el cumplimiento de las formalidades específicas requeridas para los actos jurídicos y el otorgamiento de fe pública.

Artículo 9º .- Tecnologías de firmas electrónicas al interior de la Infraestructura Oficial de Firma Electrónica

La Infraestructura Oficial de Firma Electrónica se puede basar en las siguientes tecnologías de firmas electrónicas:

a) Tecnologías de firmas digitales, sobre la cual se basa la Infraestructura Oficial de Firma Digital.

b) Otras tecnologías de firmas electrónicas que sean aprobadas por la autoridad administrativa competente de acuerdo con el principio de neutralidad tecnológica.

Artículo 10º .- Conservación de mensaje de datos o documentos electrónicos

Cuando el usuario lo solicite o la legislación exija que los documentos, registros o informaciones requieran de una formalidad adicional para la conservación de mensaje de datos o documentos electrónicos firmados electrónicamente, deberá cumplirse con lo siguiente:

a) Que sean accesibles para su posterior consulta.

b) Que sean conservados con su formato original de generación, envío, recepción u otro formato que reproduzca en forma demostrable la exactitud e integridad del contenido digital o electrónico..c) Que sea conservado todo dato que permita determinar el origen, destino,
fecha y hora el envío y recepción, en concordancia con lo establecido en el Decreto Legislativo Nº 681 y sus normas complementarias.

Cuando los documentos y mensajes de datos firmados electrónicamente sean conservados mediante microformas y almacenados en microarchivos, se sujetarán a lo dispuesto por el Decreto Legislativo Nº 681 y sus normas modificatorias y reglamentarias. El notario o fedatario responsable, que cuente con certificado o diploma de idoneidad técnica, certifica el cumplimiento de los requisitos establecidos en el presente artículo.

TÍTULO II
DE LA INFRAESTRUCTURA OFICIAL DE FIRMA DIGITAL

CAPÍTULO I
ASPECTOS GENERALES

Artículo 11º .- Elementos de la Infraestructura Oficial de Firma Digital

La Infraestructura Oficial de Firma Digital está constituida por:

a) Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente, de acuerdo con lo establecido por la autoridad administrativa competente.

b) El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal a).

c) Personal competente para la conducción de las prácticas de certificación y el mantenimiento de la Infraestructura Oficial de Firma Digital.

d) Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad,

transparencia y no-discriminación en la prestación de sus servicios.
e) Autoridad administrativa competente, así como entidades de certificación y entidades de registro o verificación debidamente acreditadas o reconocidas.

Artículo 12º .- Estándares aplicables bajo la Infraestructura Oficial de Firma Digital

Las prácticas de certificación comprendidas en la Infraestructura Oficial de Firma Digital deben estar basadas sobre los estándares técnicos internacionales vigentes que aseguren la interoperabilidad y las funciones exigidas en la Ley como en el Reglamento..La autoridad administrativa competente determinará los estándares compatibles
aplicando el principio de neutralidad tecnológica con la necesidad de cumplir los requisitos mencionados en el párrafo anterior.

CAPÍTULO II
DE LA FIRMA DIGITAL

Artículo 13º .- Firmas digitales generadas bajo la Infraestructura Oficial de Firma Digital

Las firmas digitales que gozan de las presunciones establecidas en los artículos 6º y 8º del Reglamento son las generadas a partir de certificados digitales:
a) Emitidos conforme a lo dispuesto en el Reglamento por entidades de certificación acreditadas ante la autoridad administrativa competente.
b) Incorporados a la Infraestructura Oficial de Firma Digital bajo acuerdos de certificación cruzada, conforme al artículo 49º del Reglamento.
c) Reconocidos al amparo de acuerdos de reconocimiento mutuo suscritos por la autoridad administrativa competente conforme al artículo 47º del Reglamento.
d) Emitidos por entidades de certificación extranjeras que hayan sido incorporados por reconocimiento a la infraestructura Oficial de Firma Digital conforme al artículo 48º del Reglamento.

Artículo 14º .- Características de la firma digital

Las características mínimas de la firma digital generadas bajo la Infraestructura Oficial de Firma Digital son:
a) Se genera al cifrar el código de verificación de un mensaje de datos usando la clave privada del titular del certificado digital.
b) Es única al titular de la firma digital y a cada mensaje de datos firmado por éste.
c) Es susceptible de ser verificada usando la clave pública del titular de la firma digital.
d) Su generación está bajo el control exclusivo del titular de la firma digital.
e) Está añadida o asociada lógicamente al mensaje de datos de tal manera que es posible detectar si la firma digital o el mensaje de datos ha sido alterado.

Artículo 15º .- Funciones de la firma digital

Dadas las características señaladas en el artículo anterior, técnicamente la firma digital debe garantizar:
a) Que el mensaje de datos fue enviado y firmado con la clave privada del titular de la firma digital..b) La integridad del mensaje de datos firmado digitalmente, dado que cualquier
alteración en el mensaje de datos o en la firma digital puede ser detectada.
c) Que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su clave privada, dado que ésta se mantiene bajo su control exclusivo.

Artículo 16º .- Del titular de la firma digital

Dentro de la Infraestructura Oficial de Firma Digital, la responsabilidad sobre los efectos jurídicos generados por la utilización de una firma digital corresponde al titular del certificado digital.
Tratándose de personas naturales, éstas son titulares del certificado y de las firmas digitales que se generen a partir de aquél, incluyendo las firmas digitales que genere a través de agentes automatizados.
En el caso de personas jurídicas, son éstas las titulares del certificado digital, y sus representantes los titulares de la firma digital, con excepción de las firmas

digitales que se generen a través de agentes automatizados, situación en la cual las personas jurídicas son titulares del certificado y de las firmas digitales generadas a partir de éstos.

Artículo 17º .- Obligaciones del titular de la firma digital

Las obligaciones del titular de la firma digital son:

a) Entregar información veraz bajo su responsabilidad.

b) Generar la clave privada y firmar digitalmente mediante los procedimientos señalados por la entidad de certificación.

c) Mantener el control y la reserva de la clave privada bajo su responsabilidad.

d) Observar las condiciones establecidas por la entidad de certificación para la utilización del certificado digital y la generación de firmas digitales.

Artículo 18º .- Invalidez de la firma digital

Una firma digital generada bajo la Infraestructura Oficial de Firma Digital pierde validez si es utilizada:

a) En fines distintos para el que fue extendido el certificado digital.

b) Cuando el certificado haya sido cancelado conforme a lo establecido en el Capítulo IV del presente Título.

CAPÍTULO III
DEL CERTIFICADO DIGITAL

Artículo 19º .- Requisitos para obtener un certificado digital

Para la obtención de un certificado digital el solicitante deberá acreditar lo siguiente:.a) Tratándose de personas naturales, tener plena capacidad de ejercicio de sus derechos civiles.

b) Tratándose de personas jurídicas, acreditar la existencia de la misma y su vigencia mediante los instrumentos públicos o norma legal respectivos.

Artículo 20º .- Especificaciones adicionales para ser titular de un certificado digital

Para ser titular de un certificado digital adicionalmente se deberá cumplir con:

Entregar la información solicitada por la entidad de certificación o la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de la información proporcionada, sin perjuicio de la respectiva comprobación.

En el caso de personas naturales, la solicitud del certificado digital y el registro o verificación de su identidad son estrictamente personales. La persona natural solicitante se constituirá en titular del certificado digital y de las firmas digitales que se generen.

Para el caso de personas jurídicas, la solicitud del certificado digital del cual ésta será titular y el registro o verificación de su identidad deben ser realizados a través de un representante debidamente acreditado. Conjuntamente con la solicitud debe indicarse el representante, persona natural, al cual se le asignará la facultad de generar y usar la clave privada, señalando para tal efecto las atribuciones y los poderes de representación correspondientes. Dicha persona natural será el titular de las firmas digitales. Tratándose de certificados digitales solicitados por personas jurídicas para su utilización a través de agentes automatizados, la titularidad del certificado digital y de las firmas digitales generadas a partir de dicho certificado digital corresponderá a la persona jurídica. La atribución de responsabilidad, para tales efectos, corresponde al representante legal, que en nombre de la persona jurídica solicita el certificado digital.

Artículo 21º .- Procedimiento para ser titular de un certificado digital

Para el caso de personas naturales, éstas deberán presentar una solicitud a la entidad de registro o verificación, según sea el caso; dicha solicitud deberá estar acompañada de toda la información requerida por la declaración de prácticas de certificación o en los procedimientos declarados. La entidad de registro o verificación deberá comprobar la identidad del solicitante a través de su documento oficial de identidad. La entidad de certificación cumplirá lo dispuesto en el presente artículo, en el supuesto previsto en el segundo párrafo del artículo 12º de la Ley.

En el caso de una persona jurídica, la solicitud deberá ser presentada por la persona facultada para tal fin, debiendo acreditar la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectiva,

así como las facultades del representante. Asimismo, deberá presentar toda la información requerida por la declaración de prácticas de la entidad correspondiente..

Artículo 22º .- Obligaciones del titular de certificado digital

a) Actualizar permanentemente la información proveída tanto a la entidad de certificación como a la entidad de registro o verificación, asumiendo responsabilidad por la veracidad y exactitud de ésta.
b) Solicitar de inmediato la cancelación de su certificado digital en caso de que la reserva sobre la clave privada se haya visto comprometida, bajo responsabilidad.
c) Observar permanentemente las condiciones establecidas por la entidad de certificación para la utilización del certificado digital.

Artículo 23º .- Contenido del certificado digital

Los certificados digitales emitidos dentro de la Infraestructura Oficial de Firma Digital deberán contener como mínimo lo establecido en el artículo 7º de la Ley.
La entidad de certificación podrá incluir, a pedido del solicitante del certificado digital, información adicional siempre y cuando la entidad de registro o verificación compruebe fehacientemente la veracidad de ésta.

Artículo 24º .- Período de vigencia

El período de vigencia de los certificados digitales comienza y finaliza en las fechas indicadas en él, salvo en los supuestos de cancelación conforme al artículo 9º de la Ley.

CAPÍTULO IV
DE LA CANCELACIÓN DE CERTIFICADOS DIGITALES

Artículo 25º .- Causales de cancelación del certificado digital

a) Por solicitud del titular sin previa justificación, siendo necesario para tal efecto la aceptación y autorización de la entidad de certificación o la entidad de registro o verificación, según sea el caso. La misma que deberá ser aceptada y autorizada como máximo dentro del plazo establecido por la autoridad administrativa competente, si en el plazo indicado la entidad no se pronuncia, se entenderá la cancelación del certificado; la misma que no podrá ser opuesta al tercero de buena fe.
b) Por revocatoria de la entidad de certificación, con expresión de causa.
c) Por expiración del plazo de vigencia.
d) Por el cese de operaciones de la entidad de certificación que lo emitió.
e) Por resolución administrativa o judicial que lo ordene.
f) Por interdicción civil judicialmente declarada, declaración de ausencia o de muerte presunta, del titular del certificado digital.
g) Por extinción de la personería jurídica o declaración judicial de quiebra.
h) Otras causales que establezca la autoridad administrativa competente..

Artículo 26º .- Cancelación del certificado digital a solicitud de su titular

La solicitud de cancelación de un certificado digital puede ser realizada por su titular o a través de un representante debidamente acreditado; pudiendo realizarse mediante documento electrónico firmado digitalmente, de acuerdo con los procedimientos definidos en cada caso por las entidades de certificación.
El titular del certificado digital está obligado, bajo responsabilidad, a solicitar la cancelación al tomar conocimiento de la ocurrencia de alguna de las siguientes circunstancias:
a) Por exposición, puesta en peligro o uso indebido de la clave privada.
b) Por deterioro, alteración o cualquier otro hecho u acto que afecte la clave privada.

Artículo 27º .- Cancelación por revocación

Para efectos de la cancelación de oficio o revocación de certificados digitales, la entidad de certificación debe contar con procedimientos detallados en su declaración de prácticas de certificación.
La revocación también puede ser solicitada por un tercero que informe fehacientemente de alguno de los supuestos de revocación contenidos en los numerales 1) y 2) del artículo 10º de la Ley.
La revocación debe indicar el momento desde el cual se aplica, precisando como mínimo la fecha y el tiempo del mismo, que deberá estar expresado en

minutos y segundos. La revocación no puede ser aplicada retroactivamente y debe ser notificada al titular del certificado digital. La entidad de certificación debe inmediatamente incluir la revocación del certificado en la relación que corresponda.

CAPÍTULO V
DE LA ENTIDAD DE CERTIFICACIÓN

Artículo 28º .- De las funciones de la entidad de certificación
Las entidades de certificación tendrán las siguientes funciones:
a) Emitir certificados digitales manteniendo su numeración correlativa.
b) Cancelar certificados digitales.
c) Gestionar certificados digitales emitidos en el extranjero.
d) Adicionalmente a las anteriores las señaladas en el artículo 32º del Reglamento, en caso opten por asumir las funciones de entidad de registro o verificación.
Las entidades de certificación podrán brindar otros servicios inherentes a los de certificación, cuyas características y procedimientos estarán contenidos en su declaración de prácticas de certificación..

Artículo 29º .- De las obligaciones de la entidad de certificación
Las entidades de certificación tienen las siguientes obligaciones:
a) Cumplir con su declaración de prácticas de certificación.
b) Informar a los usuarios todas las condiciones de emisión y de uso de sus certificados digitales, incluyendo las referidas a la cancelación de éstos.
c) Mantener el control y la reserva de la clave privada que emplea para firmar los certificados digitales que emite, bajo responsabilidad.
d) Mantener depósito de los certificados digitales emitidos y cancelados, consignando su fecha de emisión y vigencia.
e) Publicar permanente e ininterrumpidamente por medios telemáticos la relación de los certificados digitales emitidos y cancelados.
f) Cancelar el certificado digital a solicitud de su titular o, de ser el caso, a solicitud del titular de la firma digital; o cuando advierta que la información contenida en el certificado digital fuera inexacta o hubiera sido modificada, o que el titular incurriera en alguna de las causales previstas en el artículo 25º del Reglamento.
g) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales, limitando su empleo a las necesidades propias del servicio de certificación, salvo orden judicial o pedido expreso del titular del certificado digital.
h) Brindar todas las facilidades al personal autorizado por la autoridad administrativa competente para efectos de supervisión y auditoría.
i) Mantener la información relativa a los certificados digitales que hubieren sido cancelados, por un período mínimo de diez (10) años a partir de su cancelación.
j) Cumplir los términos bajo los cuales obtuvo la acreditación, así como los requerimientos adicionales que establezca la autoridad administrativa competente conforme a lo establecido en el Reglamento.
k) Informar y solicitar autorización a la autoridad administrativa competente para realizar acuerdos de certificación cruzada que proyecte celebrar, así como los términos bajo los cuales dichos acuerdos se suscribirían.
l) Informar y solicitar autorización a la autoridad administrativa competente para efectos del reconocimiento de certificados emitidos por entidades extranjeras.
m) Cumplir sus funciones dentro de los plazos señalados en su declaración de prácticas de certificación.
n) Contratar los seguros o garantías bancarias necesarias que permitan indemnizar al titular por los daños que pueda ocasionar como resultado de las actividades de certificación.

Artículo 30º .- Respaldo financiero
Las entidades de certificación acreditadas o reconocidas deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial.de Firma Digital, así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y en el Reglamento. La autoridad

administrativa competente definirá los criterios para evaluar el cumplimiento de este requisito.

Artículo 31º .- Del cese de operaciones de la entidad de certificación

La entidad de certificación cesa sus operaciones en el marco de la Infraestructura Oficial de Firma Digital, en los siguientes casos:

a) Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por decisión motivada de la autoridad administrativa competente.
e) Por resolución judicial.
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contemplados en los incisos a) y b) la autoridad administrativa competente establecerá el plazo en el cual las entidades de certificación notificarán tanto a aquélla como a los titulares de certificados digitales el cese de sus actividades. La autoridad administrativa competente deberá adoptar las medidas necesarias para preservar las obligaciones contenidas en los incisos d), g) e i) del artículo 29º del Reglamento.

La autoridad administrativa competente reglamentará los procedimientos para hacer público el cese de operaciones de las entidades de certificación.

Los certificados digitales emitidos por una entidad de certificación cuyas operaciones han cesado deben ser cancelados a partir del día, hora, minuto y segundo en que se aplica el cese. El uso de certificados digitales con posterioridad a su cancelación implica la pérdida de las presunciones descritas en los artículos 6º y 8º del Reglamento.

CAPÍTULO VI
DE LA ENTIDAD DE REGISTRO O VERIFICACIÓN

Artículo 32º .- De las funciones de la entidad de registro o verificación

Las entidades de registro o verificación tienen las siguientes funciones:

a) Identificar al solicitante del certificado digital mediante el levantamiento de datos y la comprobación de la información brindada por aquél.
b) Aceptar, autorizar según sea el caso, la conformidad de las solicitudes de emisión, modificación o cancelación de certificados digitales, comunicándolo a la entidad de certificación bajo responsabilidad.

Artículo 33º .- De las obligaciones de la entidad de registro o verificación

Las entidades de registro o verificación acreditadas tienen las siguientes obligaciones:

a) Cumplir los procedimientos declarados para la prestación del servicio.
b) Determinar objetivamente y en forma directa la veracidad de la información proporcionada por el solicitante de certificado digital bajo responsabilidad.
c) Mantener la confidencialidad de la información relativa a los solicitantes y titulares de certificados digitales limitando su empleo a las necesidades propias del servicio de registro o verificación, salvo orden judicial o pedido expreso del titular del certificado digital.
d) Recoger únicamente información o datos personales de relevancia para la emisión de los certificados.
e) Informar y solicitar autorización a la autoridad administrativa, especialmente en el supuesto previsto en el artículo 48º del Reglamento.
f) Acreditar domicilio en el Perú.
g) Contratar los seguros necesarios que le permitan indemnizar por los daños que puedan ocasionar como resultado de las actividades de registro o verificación.

Artículo 34º .- Respaldo financiero

Las entidades de registro o verificación acreditada deberán contar con el respaldo económico suficiente para operar bajo la Infraestructura Oficial de Firma Digital; así como para afrontar el riesgo de responsabilidad por daños, de conformidad con lo dispuesto en la Ley y por el Reglamento. La autoridad administrativa competente definirá los criterios para evaluar el cumplimiento de

este requisito.

Artículo 35º .- Del cese de operaciones de la entidad de registro o verificación

La entidad de registro o verificación cesa de operar en el marco de la Infraestructura Oficial de Firma Digital:

a) Por decisión unilateral comunicada ante la autoridad administrativa competente, asumiendo la responsabilidad del caso por dicha decisión.
b) Por extinción de su personería jurídica.
c) Por revocación de su registro.
d) Por sanción dispuesta por la autoridad administrativa competente.
e) Por orden judicial.
f) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal, o resolución judicial de quiebra.

Para los supuestos contenidos en los incisos a) y b), la entidad de registro o verificación debe notificar el cese de sus actividades a la autoridad administrativa.competente con una anticipación mínima que será establecida por ésta, debiendo dejar constancia ante aquélla de los mecanismos utilizados para preservar el cumplimiento de lo dispuesto en el inciso c) del artículo 33º del Reglamento.

TÍTULO III
DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE
CAPÍTULO I
FUNCIONES DE LA AUTORIDAD ADMINISTRATIVA COMPETENTE

Artículo 36º .- Designación y funciones

Conforme a lo establecido en el artículo 15º de la Ley, se designa al Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual (INDECOPI) como la autoridad administrativa competente.

La autoridad administrativa competente tiene las siguientes funciones:

a) Aprobar la política de certificados y la declaraciones de prácticas de certificación.
b) Acreditar entidades de certificación nacionales y reconocer a las entidades de certificación extranjeras.
c) Acreditar entidades de registro o verificación.
d) Supervisar a las entidades de certificación y a las entidades de registro o verificación, estableciendo de ser el caso las sanciones correspondientes.
e) Cancelar las acreditaciones otorgadas a las entidades de certificación y a las entidades de registro o verificación conforme a lo dispuesto en el Reglamento.
f) Publicar ininterrumpidamente la relación de entidades acreditadas.
g) Aprobar el empleo de estándares técnicos internacionales dentro de la Infraestructura Oficial de Firma Electrónica y determinar la compatibilidad de otros estándares técnicos con los estándares internacionales.
h) Formular los criterios para el establecimiento de la idoneidad técnica que deberán cumplir quienes presten servicios en las materias reguladas por la Ley y el Reglamento, así como aquellas relacionadas con la prevención y solución de conflictos.
i) Establecer los requisitos mínimos para la prestación de los servicios de certificación y los servicios de registro o verificación.
j) Impulsar la solución de conflictos por medio de la conciliación y el arbitraje.
k) Definir los criterios para evaluar la suficiencia del respaldo financiero con el que deben contar las entidades de certificación y las entidades de registro o verificación.
l) Aprobar la utilización de otras tecnologías de firmas electrónicas distintas a las firmas digitales, previa verificación del cumplimiento de los requisitos.establecidos en el artículo 2º de la Ley y regular su utilización al interior de la Infraestructura Oficial de Firma Electrónica.
m) Suscribir acuerdos de reconocimiento mutuo con autoridades administrativas extranjeras que cumplan funciones similares a las de la autoridad administrativa competente.
n) Autorizar la realización de certificaciones cruzadas con entidades de certificación extranjeras.

o) Delegar a terceros bajo sus órdenes y responsabilidad las funciones que determine.
p) Fomentar y coordinar el uso y desarrollo de la infraestructura Oficial de Firma electrónica en las entidades del sector público nacional.
q) Aprobar y regular los servicios de valor añadido al interior de la Infraestructura Oficial de Firma Electrónica.
r) Las demás que sean necesarias para el buen funcionamiento de la Infraestructura Oficial de Firma Electrónica.

CAPÍTULO II
RÉGIMEN DE ACREDITACIÓN DE ENTIDADES DE CERTIFICACIÓN Y DE LAS ENTIDADES DE REGISTRO O VERIFICACIÓN

Artículo 37º .- Acreditación de Entidades de Certificación
Las entidades que soliciten su acreditación como entidades de certificación ante la autoridad administrativa competente deben contar con los elementos de la Infraestructura Oficial de Firma Digital señalados en los incisos a), b), c) y d) del artículo 11º, y someterse al procedimiento de evaluación comprendido en el artículo 41º del Reglamento.
Cuando alguno de los elementos señalados en el párrafo precedente sea administrado por un tercero, la entidad solicitante deberá demostrar su vinculación con aquél, asegurando la viabilidad de sus servicios bajo dichas condiciones, y la disponibilidad de estos elementos para la evaluación y supervisión que la autoridad administrativa competente considere necesarias.
La autoridad administrativa competente, de ser el caso, precisará los términos bajo los cuales se rigen estos supuestos del servicio de certificación.
Artículo 38º .- Presentación de la solicitud de acreditación de entidad de certificación
La solicitud de acreditación de entidades de certificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando lo siguiente:
a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante..b) Acreditar domicilio en el país.
c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
d) Declaración de prácticas de certificación y documentación que comprenda el sistema de gestión implementado conforme a los incisos a) y d) del artículo 11º del Reglamento.
e) Declaración jurada del cumplimiento de los requisitos señalados en los incisos b) y c) del artículo 11º del Reglamento; información que será comprobada por la autoridad administrativa competente.
f) Documentación que acredite el cumplimiento de lo dispuesto en los artículos 29º y 30º del Reglamento y demás que la autoridad administrativa competente señale.
g) Informe favorable de la entidad sectorial correspondiente, cuando lo solicite la autoridad administrativa competente, para el caso de personas jurídicas supervisadas, respecto de la legalidad y seguridad para el desempeño de actividades de certificación.
Artículo 39º .- Acreditación de Entidades de Registro o Verificación
Las entidades que soliciten su acreditación como entidades de registro o verificación ante la autoridad administrativa competente deben contar con procedimientos para la prestación de sus servicios, los mismos que tendrán que asegurar la verificación directa de la identidad del solicitante.
Artículo 40º .- Presentación de la solicitud de acreditación de Entidades de Registro o Verificación
La solicitud para la acreditación de entidades de registro o verificación debe presentarse a la autoridad administrativa competente, observando lo dispuesto en el artículo anterior y adjuntando la información y documentos siguientes:

a) Acreditación de la existencia y vigencia de la persona jurídica mediante los instrumentos públicos o norma legal respectivos, así como las facultades del representante.
b) Acreditar domicilio en el país.
c) Declaración jurada de contar con la infraestructura e instalaciones necesarias para la prestación del servicio, así como la declaración jurada de aceptación de la visita comprobatoria de la autoridad administrativa competente.
d) Procedimientos detallados que garanticen el cumplimiento de las funciones establecidas en el Reglamento.
e) Declaración de prácticas de verificación o registro.
f) Declaración jurada del cumplimiento de los requisitos señalados en los artículos 33º y 34º del Reglamento.

Artículo 41º .- Procedimiento Administrativo de la Acreditación

Admitida la solicitud, la autoridad administrativa competente procederá a la evaluación del cumplimiento de los requisitos establecidos en la Ley como en el Reglamento.
La evaluación de los requisitos de competencia técnica de la entidad de certificación o de registro o verificación solicitante podrá ser realizada directamente por la autoridad administrativa competente, o a través de terceros, o reconociendo aquéllas realizadas en el extranjero por otras autoridades extranjeras que cumplan funciones equivalentes a las de la autoridad administrativa competente, y siempre que los requisitos evaluados por ellas sean equivalentes a los requisitos comprendidos en el Reglamento.

Artículo 42º .- Reconocimiento de evaluaciones en el extranjero

La autoridad administrativa competente reconocerá las evaluaciones sobre los requisitos de competencia técnica de la entidad de certificación solicitante realizadas en el extranjero siempre y cuando se cumplan con las normas establecidas por la autoridad administrativa competente en el marco del Reglamento.

Artículo 43º .- Subsanación de observaciones

Dentro del procedimiento podrán subsanarse las deficiencias técnicas observadas durante la evaluación. La entidades podrán solicitar la suspensión del procedimiento a fin de implementar las medidas necesarias para superar estas dificultades.
Si culminada la etapa de evaluación, se mantienen observaciones, se denegará el Registro y se archivará el procedimiento.

Artículo 44º .- Costos del Registro y otros procedimientos

Las entidades solicitantes asumirán los costos por la tramitación del procedimiento, y aquellos por evaluación, auditoría y demás previstos por la autoridad administrativa competente.

Artículo 45º .- Otorgamiento y vigencia de la Acreditación

La acreditación se otorga por un período de 10 años, renovables por períodos similares. Durante dicho período la Entidad beneficiaria estará sujeta a evaluaciones técnicas anuales para mantener la vigencia de la referida acreditación.

Artículo 46º .- Cancelación de la Acreditación

La cancelación de la acreditación procede por:
a) Solicitud de la entidad de certificación o de la entidad de verificación o registro.
b) Extinción de su personería jurídica.
c) Sanción impuesta por la autoridad administrativa competente o por decisión judicial.
d) Por liquidación, decidida por la junta de acreedores en el marco de la legislación concursal o resolución judicial de quiebra.

CAPÍTULO III
DE LOS CERTIFICADOS EMITIDOS POR ENTIDADES EXTRANJERAS

Artículo 47º .- Acuerdos de reconocimiento mutuo

La autoridad administrativa competente podrá suscribir acuerdos de reconocimiento mutuo con entidades similares, a fin de reconocer la validez de certificados digitales otorgados en el extranjero y extender la validez de la

Infraestructura Oficial de Firma Digital. Los acuerdos de reconocimiento mutuo deben garantizar en forma equivalente las funciones exigidas por la Ley como en el Reglamento.

Artículo 48º .- Reconocimiento de certificados emitidos por entidades extranjeras

La autoridad administrativa competente podrá reconocer certificados digitales emitidos por entidades extranjeras, de acuerdo con las prácticas y políticas que para tal efecto apruebe, las mismas que deben velar por el cumplimiento de las obligaciones y responsabilidades establecidas en el Reglamento u otra norma posterior. Asimismo, podrá autorizar la operación de aquellas entidades de certificación nacionales que utilicen los servicios de entidades de certificación extranjera, de verificarse tal supuesto, las entidades nacionales asumirán las responsabilidades del caso.

Para los efectos de lo dispuesto en el párrafo precedente, la entidad extranjera deberá comunicar a la autoridad administrativa competente el nombre de aquellas entidades de certificación que autorizarán las solicitudes de emisión de certificados digitales así como la gestión de los mismos.

La autoridad administrativa competente emitirá las normas que aseguren el cumplimiento de lo establecido en el presente artículo; así como los mecanismos adecuados de información a los agentes del mercado.

Artículo 49º .- Certificación cruzada

Las entidades de certificación acreditadas pueden realizar certificaciones cruzadas con entidades de certificación extranjeras a fin de reconocer los certificados digitales que éstas emitan en el extranjero incorporándolos como suyos dentro de la Infraestructura Oficial de Firma Digital de conformidad con el artículo 11º de la Ley, siempre y cuando obtengan autorización previa de la autoridad administrativa competente.

Las entidades que presten servicios de acuerdo a lo establecido en el párrafo precedente, asumirán responsabilidad de daños y perjuicios por la gestión de tales certificados.

Las entidades de certificación acreditadas que realicen certificaciones cruzadas conforme al primer párrafo del presente artículo, garantizarán ante la autoridad administrativa competente que los certificados digitales reconocidos han sido emitidos bajo requisitos equivalentes a los exigidos en la Infraestructura Oficial de Firma Digital, y que cumplen las funciones señaladas en el artículo 2º de la Ley.

CAPÍTULO IV
SUPERVISIÓN DE ENTIDADES ACREDITADAS

Artículo 50º .- Facultades de Supervisión

La autoridad administrativa competente tiene la facultad de verificar la correcta prestación de los servicios de certificación así como de los servicios de registro o verificación y el cumplimiento de las obligaciones legales y técnicas por parte de las entidades acreditadas que operen bajo la Infraestructura Oficial de Firma Electrónica, así como la facultad de verificar el cumplimiento de las disposiciones establecidas en la Ley, el Reglamento, y en sus Resoluciones.

DISPOSICIONES FINALES

Artículo Primero.- Las entidades del Sector Público Nacional pueden suscribir acuerdos de cooperación con sus similares a nivel mundial o con instituciones de cooperación, para recibir apoyo, asesoría y financiamiento para el desarrollo del comercio electrónico en general, las firmas electrónicas y las firmas y certificados digitales en particular.

Artículo Segundo.- Las entidades de certificación deben establecer procedimientos ágiles y sencillos para que sus usuarios puedan presentar directamente reclamaciones por la prestación de sus servicios, las mismas que deberán ser atendidas en el más breve plazo. La autoridad administrativa competente aprueba o reforma estos procedimientos y regula todo lo relativo a las reclamaciones. Agotada la vía previa de la reclamación ante la entidad de

certificación, procede recurrir en vía administrativa ante la autoridad administrativa competente, con sujeción a la Ley Nº 27444 - Ley del Procedimiento Administrativo General.
La autoridad administrativa competente determinará todos aquellos procedimientos y políticas necesarios para la aplicación del Reglamento. En los casos que proceda la reclamación, adoptará las medidas correctivas pertinentes.